PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
RL.P52960WO		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP 03/51101	24.12.2003	24.12.2003
International Patent Classification (IPC) or both national classification and IPC		
INV. H04Q7/38 H04Q7/32 H04L29/06		
Applicant		
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) et al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the opinion
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
04.11.2005	31.03.2006
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Matt, S Telephone No. +49 89 2399-7638

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP 03/51101

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1-11	as originally filed

Claims, Numbers

1-28	received on 25.11.2005 with letter of 21.11.2005
29, 30	filed with telefax on 21.03.2006

Drawings, Sheets

1/2, 2/2	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   ☐ the language of publication of the international application (under Rule 48.3(b)).

   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority in written form.

   ☐ furnished subsequently to this Authority in computer readable form.

   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:

   ☐ the claims, Nos.:

   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-27,29
	No:	Claims	28,30
Inventive step (IS)	Yes:	Claims	1-27,29
	No:	Claims	28,30
Industrial applicability (IA)	Yes:	Claims	1-30
	No:	Claims	

2. Citations and explanations

   see separate sheet

Cited Documents

1. Reference is made to the following documents:

D1: XP-A-002292895 (On the Security of Wireless Network Access with Enhancements)

Re Item V
Reasoned statement under Rule 66.2 (a) (ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

A. Novelty / Inventive Step (Article 33 PCT):

1. re independent **Claim 28**:

The subject-matter of independent **claim 28 (mobile wireless terminal) is not novel** in the sense of Article 33 (2) PCT for the following reasons:

Document D1 discloses all features of claim 28 (references in parentheses applying to this document):

A mobile wireless terminal (*D1, MS, figure 3*), the terminal comprising

- means for generating and storing a first numerical chain comprising a series of n values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value (*D1, hash chaining, $f^M(x)= f(f(...f(x)...))$; chapter 5.2, left column*); and

- means for disclosing values from the numerical chain to an access node (*D1, "claimant... sends fM(b)... to the verifier", chapter 5.2, left column; "... The MS and the old VLR can still keep their old authentication states...", page 94, left column, last bullet item*) in order to allow the access node to authenticate the mobile wireless terminal (*D1, "the verifier checks the equality f (f M-1(b))=fM(b)", chapter 5.2, left column*) .

As a consequence, the subject-matter of **claim 28 lacks novelty** in the light of the disclosure of document D1 (Article 33 (2) PCT).

2. re independent **Claim 30**:

The subject-matter of independent **apparatus claim 30 (control node)** represents the peer unit of the mobile wireless terminal according to claim 28 and does not add any additional technical features. For the reasons set out in the previous subsection and the fact that D1 discloses the authentication process performed in the VLR (D1, figure 3) which is considered as a control node, the **subject-matter** of said **claim lacks novelty** (Article 33 (2) PCT).

3. The subject-matter of the application relates to **a method (claim 1)** of authenticating a mobile node in a communication system comprising a plurality of access nodes. The authentication is based on chained hash-values. Furthermore it relates to a corresponding **access node (claim 29).**

3.1 **Document D1** discloses inter-alia an enhanced UMTS-AKA mechanism based on a one-way hash chaining algorithm. The MS and the HLR share a common secret seed. A hash value chain is then derived from that seed

i.e. $hash^M(seed) = hash(hash(hash(hash(hash...hash(seed))...))$ whereas M corresponds to the number of the application of the hash operation.

This hash chain can be used to verify the authenticity of a mobile station M times. During the first visit the mobile station to be authenticated sends the second last value $(hash^{M-1})$ to the verifier. The verifier compares this value after applying an additional hash operation on it with the pre-stored value ($hash^M$). After successful authentication the pre-stored value is replaced by value latest received value ($hash^{M-1}$) used for the next future authentication request.

In case of roaming, a new set of hash values (chain) is agreed between the mobile station and the new VLR involving the HLR for the initial authentication.

No indication is given in the cited document D1 to provide all access-nodes of the

communication system with the updated hash-chain value received from the last serving access-node which is needed for performing successfully the next authentication.

3.2. The technical problem addressed by the subject-matter of the independent claims is to provide a fast handover/roaming mechanism whereas authentication is required.

3.3 This problem is solved by generating initially a value chain using one way coding functions which are used for authentication. A given value in the chain is easily obtainable from a subsequent value by applying the one way coding function but the subsequent value is not easily obtainable from that given value; authentication is performed sending a value from the chain to the access node. The predecessor value already sent previously to the access node is hashed in order to compare it with the value received from the mobile device; in case of conformance the mobile device is authenticated. Afterwards, the received value is distributed to the other access nodes.

3.4 This method ensures a high secure and fast authentication in case of handover/roaming thereby reducing the signalling load to the HLR in respect of authentication.

3.5. The proposed solution as defined by the subject-matter of the independent claims is not taught, suggested or derivable by the available prior art documents.

3.6 **The subject-matter of the independent claims 1 and 29 is therefore considered to be new and to involve an inventive step, Article 32 (2) and (3) PCT. As a consequence, the dependent claims also meet the requirements of Article 32 (2) and (3) PCT. The claims are also considered as industrially applicable, Article 32 (4).**

B. Deficiencies with respect to clarity (Article 6 PCT):

1. Independent **claim 29** does not meet the requirement following from Article 6 PCT taken in combination with Rule 6.3(b) PCT that any independent claim must contain all technical features essential to the definition of the invention. It is considered as

essential, that the surrounding access nodes are provided with knowledge of the latest used value. Contrary to claim 1 which defines

> "*... the sent value preceding values in the chain already sent to the access nodes...*"

no indication is given in claim 29, that the access node receives the preceding value in the chain from another node. The mere notification of a previously performed successful authentication is not sufficient.

C. Further deficiencies

1. The independent claims are not in the two-part form in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art being placed in the preamble (Rule 6.3(b)(I) PCT) and with the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).

2. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

CLAIMS:

1. A method of authenticating a mobile node to a communication system, the communication system comprising a plurality of access nodes between which the mobile node is able to roam, the method comprising:

(a) generating a numerical chain comprising a series of values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value;

(b) each time that the mobile node seeks to authenticate itself to an access node, sending a value from the numerical chain from the mobile node to an access node to which the mobile node wishes to attach, the sent value preceding values in the chain already sent to access nodes; and

(c) using the sent value at the access node to authenticate the mobile node on the basis of a value of the numerical chain preceding the sent value in the chain,

the method further comprising, after each successful authentication, informing each of said plurality of access nodes that an authentication has been completed.

2. A method according to claim 1, wherein the comparison of the sent value and an earlier value of the numerical chain comprises comparing the output of the one-way coding function applied at least once to the sent value to an earlier value of the numerical chain.

3. A method according to any preceding claim, wherein the earlier value of the numerical chain is the value immediately preceding the sent value.

4. A method according to any preceding claim, wherein the authenticating node is the access node to which the mobile node wishes to attach.

5. A method according to claim 4, wherein the authenticating node sends a notification update to the remainder of the plurality of access nodes upon successful authentication of the mobile node.

6. A method according to claim 5, wherein the update notification is issued through a secure local multicast mechanism.

7. A method according to any one of claims 1 to 3, wherein the authenticating node is a control node which communicates with the plurality of access nodes.

8. A method according to claim 7, wherein the authenticating node stores an update notification upon successful authentication of the mobile node.

9. A method according to claim 5 or 8, wherein the notification update comprises the sent value provided by the mobile node.

10. A method according to any preceding claim, wherein a value H_{i-1} of the numerical chain may be obtained from a value H_i of the numerical chain using the one-way coding function defined such that $H_{i-1} = \mathtt{hash}(H_i)$.

11. A method according to any preceding claim, wherein the numerical chain is generated by providing a seed value H_n of the numerical chain, all subsequent values being obtainable through successive application of the one-way coding function.

12. A method according to claim 11, wherein the seed value H_n is based upon a value known only to the mobile node and a home network.

13. A method according to claim 11, wherein the seed value H_n is based upon a value known only to the mobile node.

14. A method according to any one of claims 11 to 13, wherein the seed value H_n is based upon the EAP MSK or EMSK value.

15. A method according to any one of claims 11 to 13, wherein the seed value H_n is based upon a randomly generated value.

16. A method according to any one of claims 11 to 15, wherein the seed value is encrypted so that the access nodes cannot determine the seed value.

17. A method according to any preceding claim, wherein the first value of the numerical chain, obtained from successive applications of the one-way coding function to a seed value, is provided to the authenticating node by either the mobile node or a home network to which the mobile node is subscribed.

18. A method of authenticating a mobile node to a communication system, the communication system comprising a plurality of access nodes and a plurality of interfaces, the method comprising generating a plurality of numerical chains, each of the plurality of numerical chains corresponding to one of the plurality of interfaces, and

authenticating the mobile node on a plurality of the interfaces in accordance with the method of claim 1.

19. A method according to claim 18, wherein the mobile node authenticates itself to the plurality of interfaces in parallel.

20. A method according to any preceding claim, wherein a value of the numerical chain is used to generate at least part of an IP address for the mobile node.

21. A method according to any preceding claim, wherein each numerical chain is bound to a specific MAC address corresponding to a specific access node.

22. A method according to any preceding claim, wherein the communication system comprises a wireless access network, and the mobile node is a wireless terminal.

23. A method of authenticating a mobile node when roaming within a communication system, the method comprising:

following handover of the mobile node from a first access node of the communication system to a second access node, authenticating the mobile node to the second access node using the method of any one of the preceding claims.

24. A method according to claim 23, wherein the mobile node has been previously authenticated to the said communication system by a home network of the mobile node.

25. A method of deriving a secure authentication key when a mobile node authenticates itself to an access node in accordance with any preceding claim, the method comprising:

providing a first authentication key K_{S0} for use by the mobile node and a first access node;

sending a hash of the first authentication key $\mathtt{hash}(K_{S0})$ to a second access node and the mobile node; and

generating a new authentication key K_{S1} in accordance with the hash $\mathtt{hash}(K_{S0})$.

26. A method according to claim 25, wherein the new authentication key is generated by taking a hash of the hash $\mathtt{hash}(K_{S0})$, in accordance with the function $K_{S1} = \mathtt{hash}(\mathtt{hash}(K_{S0}))$.

27. A method according to claim 25, further comprising the steps of:

exchanging a first nonce N_{C1} provided by the mobile node and a second nonce N_{A1} provided by the second access node between the mobile node and the second access node; and wherein the new authentication key K_{S1} is generated in accordance with the hash of the first session key K_{S0}, the first nonce N_{C1} and the second nonce N_{A1} in accordance with the function $K_{S1} = \mathtt{hash}(\mathtt{hash}(K_{S0}), N_{C1}, N_{A1})$.

28. A mobile wireless terminal, the terminal comprising means for generating and storing a first numerical chain comprising a series of n values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for disclosing values from the numerical chain to an access node in order to allow the access node to authenticate the mobile wireless terminal.

29. An access node of a communication system having: means for receiving from another node of the communication system a notification each time a mobile node has been successfully authenticated by the communication system; means for receiving from a mobile node a value of a first numerical chain comprising a series of n values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for authenticating the mobile node on the basis of that value and the previously received notifications.

30. A control node of a communication system having means for receiving from a mobile node or an access node a value of a first numerical chain comprising a series of n values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for authenticating the mobile node on the basis of that value.